Computer Communications 164 (2020) 50–53

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Editorial

Deep learning for intelligent IoT: Opportunities, challenges and solutions

Yousaf Bin Zikria [a], Muhammad Khalil Afzal [b], Sung Won Kim [a,*], Andrea Marin [c], Mohsen Guizani [d]

[a] Department of Information and Communication Engineering, Yeungnam University, 280 Daehak-Ro, Gyeongsan 38541, Republic of Korea
[b] COMSATS University, Islamabad, Wah Campus, Wah Cantt 47010, Pakistan
[c] Università Ca' Foscari Venezia, Torino 155, 30172, Venice, Italy
[d] University of Idaho, USA

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Machine learning
Deep learning
Reinforcement learning
Network protocols
Network security
Health-based IoT
Industrial Internet of Things (IIoT)
Intelligent Transportation System (ITS)
Big data

ABSTRACT

Next-generation wireless networks have to be robust and self-sustained. Internet of things (IoT) is reshaping the technological adaptation in the daily life of human beings. IoT applications are highly diverse, and they range from critical applications like smart city, health-based industries, to industrial IoT. Machine learning (ML) techniques are integrated into IoT to make the network efficient and autonomous. Deep learning (DL) is one of the types of ML, and it is computationally complex and expensive. One of the challenges is to merge deep learning methods with IoT to overall improve the efficiency of the IoT applications. An amalgamation of these techniques, maintaining a balance between computational cost and efficiency is crucial for next-generation IoT networks. In consideration of the requirements of ML and IoT and seamless integration demands overhauling the whole communication stack from physical layer to application layer. Hence, the applications build on top of modified stack will be significantly benefited, and It also makes it easy to widely deploy the network.

1. Introduction

Wireless networks of the future generation are required to enable ultra-reliable and low latency communications. Artificial intelligence (AI) has flourished in recent years through developments in machine learning (ML), especially in deep learning (DL) and reinforcement learning (RL), showing its usefulness in a wide variety of applications where classification or regression problems play a key role [1]. One of the key-applications of future-generation wireless networks is the management of the Internet of things (IoT) infrastructures. The deployment of wireless networks enabling the IoT paradigm, is gaining more attention from academic as well as industrial researchers. The complexity and pervasive nature of these systems raise many challenges that include the design and integration of heterogeneous communication systems, the dynamic adaptation to different working scenarios, and the capability of information extraction from massive data collected and transmitted by sensors [2]. This type of system's dynamic, heterogeneous, and distributed nature led many researchers and practitioners to explore the application of DL techniques to render IoT intelligent, reliable, and high-performance. Forbes predicted that IoT industry would grow to $457 billion by 2020. The main contributors to this major adaptation and development are the smart cities, smart grid , smart health, and industrial IoT (IIoT). The transition known as Industry 4.0 precisely takes immense advantage of advances in the field of IoT.

IoT systems consist of a large number of distributed heterogeneous devices producing a consistent volume of data. Obviously, in this context, wireless solutions are of primary importance, as evidenced by the rapid production of industrial (often low-cost) components which have helped to actually incorporate this technology. Data harvested by the devices is progressively increasing in size and heterogeneity. In fact, IoT networks are fundamentally diverse and dynamic. Algorithms designed for networks with partial standardized features are not typically efficient once applied to IoT systems [3]. Finally, IoT devices often have limited computing, memory, and energy resources so they rely heavily on edge and core networks to manage, process, and analyze data. As a result, DL-based edge and core devices are vital to the development of intelligent and effective resource management and network management and the enhancement of system efficiency overall. Indeed, a fundamental field of research is the quantitative evaluation and optimization of an IoT system: wireless traffic is increasing exponentially with the continuous increase in the number of IoT devices producing large short-packet transmissions over wireless downlink/uplink. For these reasons, communication protocols must also adapt to such a complex real-time IoT environment. With regard to ordinary wired and wireless networks, IoT networks typically need optimization in terms

* Corresponding author.
E-mail addresses: yousafbinzikria@gmail.com (Y.B. Zikria), khalilafzal@ciitwah.edu.pk (M.K. Afzal), swon@yu.ac.kr (S.W. Kim), marin@unive.it (A. Marin), mguizani@uidaho.edu (M. Guizani).

https://doi.org/10.1016/j.comcom.2020.08.017

Available online 27 August 2020

of their energy usage and load-balancing techniques that need to be developed for the stable operation of IoT devices for several years [4].

The heterogeneity of the IoT systems also poses questions about interoperability from the practical point of view. Anomaly detection and protection are also one of the industry's immense challenges: shielding the infrastructure from malicious network attacks, unauthorized access, and safeguarding user privacy are important and daunting criteria at the same time. The anomaly detection systems , for example, need adaptation to unexpected events in order to account for the largest class of cyber threats. The developments seen in the last decade in the field of AI have attracted the interest of researchers in communication networks and created a fertile area of interdisciplinary research [5]. Intelligent IoT includes tackling all the enormous challenges described above. Without human interference DL aims to solve such a wide set of problems.

The remainder of this editorial is organized as follows. Section 2 provides future research directions. Section 3 summarizes the accepted papers. Finally, Section 4 concludes the editorial.

2. Future research directions

AI, and specifically DL, supports the creation of dynamic IoT systems both on the design of the communication infrastructure and on the analysis of data. From the design point of view, the highly distributed nature of IoT wireless systems, the heterogeneity of the low-cost devices that they consist of (and hence the lack of programmable centralized devices) make traditional approaches to Quality of Service (QoS) and security control unfeasible. However, the large amount of data collected by IoT systems allows for the training of neural networks that can control the performance and security of the system. Both of these aspects require further attention from academic and industrial researchers. In fact, QoS does not only impact the users' experience but also plays a pivotal role in the management of emergency of critical scenarios. These require the devices to be able to distinguish among the high-priority, emergency-related traffic and the regular traffic, and to privilege the former. The reliable prioritization of network traffic and usage of the networking devices to meet certain QoS standards is still, for a large part, an open problem that DL can address with potentially important results.

Aside from this example, DL applications must be investigated in the whole communication stack, from the physical level where signal encoding, aggregation, and disaggregation of channels may be decided thanks to AI models, in contrast with the traditional explicit optimization approach, to the application level, as we will discuss later. Also, the network layer requires novel techniques for deciding and adapting routing algorithms that may be totally or partially unaware of the network topology and state. Indeed, the growth of IoT networks is often uncontrolled, and the conditions of certain areas are highly unpredictable. AI will help in the design or proactive reactive mechanisms aimed at guaranteeing the minimum QoS even in case of anomalies.

The security of IoT systems is another field that will draw many research efforts in the next years. While traditional cryptographic based protocols are often unusable in IoT systems due to the low computational power of the devices they consist of, the demand for secure infrastructures, both from the point of view of the confidentiality and on the communication reliability, needs an urgent answer. The application of DL to intrusion detection in IoT networks has lead to some interesting contributions in the scientific literature. However, still, ample space for improvements and further directions remains to be explored, including the preservation of confidentiality, the resilience to attacks that undermine parts of the communication infrastructure (e.g., jamming attacks), and so on.

The probably largest area for future deployment of DL in IoT remains the high-level applications, i.e., the analytics of IoT harvested data. The growing spread of IoT devices allows for a high number of case studies aimed at making our societies more inclusive, secure and, in general, smart.

In the next decades, one of the crucial challenges that many societies will have to face is the population aging and the consequent distributed assistance and monitoring that many elders, vulnerable and possibly nonautonomous citizens will require. Reliable and secure IoT systems equipped with AI is the main route to diffuse monitoring of people in need of attention, detection of anomalies (e.g., strokes, falls, blood pressure issues) and providing information for a higher quality of life (e.g., computation of pedestrian routes without architectural barrier).

The quality of life in our cities does not depend only on the inclusion of more vulnerable people. Ensuring security in public places such as big events, public transportation systems, schools, and universities is a growing concern in nowadays societies. AI systems can use multimedia data coming from sensors of IoT networks to perform anomaly detection and prevent terrorist attacks or violent crimes. In general, while DL techniques have enabled these tasks, the integration with IoT still requires further development. The high bandwidth required by multimedia streams and the QoS strict requirements of these types of applications pose serious problems to the current IoT infrastructures, and further developments, both from the theoretical and practical points of view, are required.

The other challenge that societies must urgently face is the mitigation of the causes of climate change. While high-level policies decided by Governments play a central role to this aim, doubtless the change of habits of millions of people in the direction of a more sustainable lifestyle can have a high impact on the reduction of carbon dioxide and preservation of non-renewable resources. IoT systems and AI can work together to learn people's habits and recommend sustainable lifestyles to the users as well as to monitor local and global environmental indices such as air pollution, glacier melting, etc. In the latter cases, the high predictive power of DL-based models trained with data coming from sensors can find novel and useful applications.

3. A brief review of accepted articles of this special issue

In this Special Issue, we have collected papers that explore the application of DL to healthcare, transportation, climate change, security and privacy, and medium access control.

Rapid global climate change demands a change in the human habitat. To tackle this problem, new innovative technologies are required to monitor the environment constantly and accordingly take appropriate actions. ML techniques can be used to make system adaptive and robust. IoT devices deployment in remote locations operate with limited battery, and it is assumed to work uninterruptedly for many years. Thippa et al. [6] used deep neural networks based techniques to efficiently collect data from multiple sensors and monitor the battery status of devices. The proposed scheme pre-processed using attribute mean method. Afterward, it is converted using the standard scalar method. The retrieved features are reduced using principal component analysis (PCA) to decrease time complexity. As it also removes negative impact features; consequently, it increases prediction accuracy. The proposed method shows improvement in terms of battery life prediction as compared to linear regression and xgboot. The proposed scheme could be enhanced further for other real-time IoT deployment scenarios, and it would be interesting to see the results when combining with bio-inspired algorithms.

Health-based IoT is one of the most critical area of research. Internet of medical things (IoMT) is the network of medical devices and humans. Advancements in IoMT will improve patients medical care service, and cheaper technology deployment will revolutionize the industry. It will be more useful to monitor patients from remote locations and provide treatment in case of any emergency. However, the challenges of providing the utmost reliable detection, communication, and processing are still at large. Al-Turjman et al. [7] studied the IoMT related papers, gave the summary, highlighted the challenges, and discussed the comprehensive future research directions. The authors categorize the IoMT framework into data acquisition, communication technologies, and post-processing technologies. The data acquisition mostly rely on wearable and non-wearable sensors. These healthcare sensors should provide accurate readings and cost effective to reduce the workload of caregivers and decrease overall healthcare costs significantly. Reliable communications technology is crucial to provide reliable services. At last, post-processing involves storing, visualizing, tracking, monitoring the patients. It could be enhanced by making it intelligent by detecting any abnormality in patients and alerting the relevant services to timely take appropriate action to save a life.

IoT devices are deployed in a large number of quantities, and it uses various communications technologies like 5G, Wi-Fi, etc. Physical layer communication security is essential to keep secrecy from an eavesdropper. Haider et al. [8] proposed an optimized secrecy rate scheme for wireless information to protect against eavesdropping attacks. They used additional noise for reliable, secure communication and wireless energy transferred. The beamforming matrix and power splitting ratio make the objective function non-convex. Hence, they proposed a concave–convex procedure (CCCP) to optimize the secrecy rate. They also utilized second-order cone programming (SOCP) to solve the iterative problem in the CCCP algorithm. The simulation results prove that the proposed scheme is superior to some other schemes in the literature. The proposed scheme can be integrated for mm-Wave, non-orthogonal multiple access techniques (NOMA) and tactile internet.

With the growth of the IoT, several devices can be connected to the network. Industrial IoT (IIoT) serves as a modern concept of IoT in the industrial sector by automating intelligent objects for sensing, capturing, storing, and interacting in industrial systems real-time events. Machine Learning can be used to improve system efficiency, productivity , and performance. Surveillance is important for system fault detection and optimization in the electric railway industry. Therefore, authors in [9] suggested a multifunctional fusion network-based scheme to enhance the efficiency and visual impact of catenary images in the railway sector. The coarse and the fine features of the images are abstracted in their proposed work and fused to know the map of transmission. The transmission map is improved in the next step , in order to maintain the edges. Results suggest that the proposed approach will enhance catenary image transparency and visual effect.

Biological data is increasing at an unprecedented pace, due to the advent of emerging sensors and high-throughput communication technologies. Biological data is distributed in complexity and geography, and available in different forms and formats. Irshad et al. [10] introduced a probabilistic model based on IoT, using Biological Data Deep Learning. The proposed framework uses deep-learning model state, and temporary knowledge processing constructs from Recurrent Neural Network (RNN) and Long Short Term Memory (LSTM). The theoretical solution considers the historical and present state of the program continuously. It probabilistically analyzes it for providing device or its creator with intelligence to upgrade the existing processes of caching, persistence, and computing. Results show that the scheme proposed for continuous optimization is efficient than optimization technique based on contextual and functional background data, autonomous and loopback mechanism.

To access the channel in wireless networks, Medium Access Control (MAC) resource allocation system uses a distributed coordinating function (DCF)-based carrier sensing multiple access with collision avoidance (CSMA/CA) mechanism. At the other hand, the Long Term Evolution (LTE) model uses a constant, minimally gaped data transmission. Hence, to ensure the fair coexistence challenge between LTE Licensed Assisted Access (LAA) and Wi-Fi listen before talk mechanism is adapted in wireless communications networks. In [11], Ali et al. proposed a reinforcement learning-enabled listen before talk mechanism for efficient and fair coexistence of long term evolution and Wi-Fi. Their proposed protocol incorporates a channel collision probability as a reward function for the fair utilization of channels in LTE-LAA and WiFi. The proposed scheme improves fairness and throughput and hence it improves the performance of overall system.

A huge amount of data is produced by the rapid adoption and evolution of IoT in healthcare, video surveillance, and transportation. For example, when used in hospital surveillance situations, IoT devices such as cameras do large amounts of photographs. An integral factor in security systems is facial recognition. Masud et al. [12] proposed smart face recognition in the IoT-cloud environment, based on DL. They presented a model of a single and parallel tree. A volume of inputs is split into multiple volumes in their proposed model, where a tree is created for each volume. A tree is defined by the factor and height of its branch. A residual function determines the branch, comprising a convolutionary layer, batch normalization, and a non-linear function. The proposed models achieved approximately 99% percent accuracy over the publicly available face databases.

IoT has revolutionized the medical field by making data collection simpler using various IoT devices. The IoT devices produce data in a specific form, including text, pictures, and videos. In medical applications, however, the data produced is in the form of images. The mining of accurate and useful knowledge from data produced by the immense serge IoT is a very challenging task. Authors in [13] proposed a cascaded approach to fully automated segmentation of brain tumors using images produced by IoT. They intelligently combine the handmade feature-based technique with the Convolutionary Neural Network for segmentation of the brain tumors. The proposed method produces promising results on a complete, core and enhancing tumor with Dice similarity scores of 0.81, 0.76, and 0.73, respectively.

To address the shortcomings of IoT security data processing with big data technology and deep learning algorithms, Amanullah et al. in [14] presented the state-of-the-art research focused on deep learning, big data technologies, and IoT security. Determining the technological applicability and limitation of deep learning, big data technology, and IoT security is the main motivation of this paper. Limitations of current approaches are evaluated, and guidelines are suggested to facilitate the successful implementation of deep learning, big data technology, and IoT security for potential researchers. In addition , the authors addressed instances of IoT security usage where deep learning and Big Data technology may be a possible solution.

4. Conclusions

Nine papers in this special issue (SI) reflect the state-of-art research trends in the domain of DL for IoT. They covers various topics that include climate change, health-care, network security, and coexistence network technologies. The accepted papers highlight key challenges and propose novel ideas to tackle these issues. The guest editors would like to thank all the authors and reviewers for their constructive and valuable contributions to this SI. We would also like to thank Carla Fabiana Chiasserini, Editor-in-Chief, for her invaluable help and productive advice in finalizing this SI.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] R. Ali, A. Nauman, Y.B. Zikria, B.-S. Kim, S.W. Kim, Performance optimization of qos-supported dense WLANs using machine-learning-enabled enhanced distributed channel access (MEDCA) mechanism, Neural Comput. Appl. (2019) http://dx.doi.org/10.1007/s00521-019-04416-1.

[2] H.S.Z. Kazmi, N. Javaid, M. Awais, M. Tahir, S.-o. Shim, Y.B. Zikria, Congestion avoidance and fault detection in WSNs using data science techniques, Trans. Emerg. Telecommun. Technol., e3756–e3756 ett.3756. http://dx.doi.org/10.1002/ett.3756.

[3] F. Al-Turjman, E. Ever, Y.B. Zikria, S.W. Kim, A. Elmahgoubi, SAHCI: Scheduling approach for heterogeneous content-centric IoT applications, IEEE Access 7 (2019) 80342–80349.

[4] A. Saleem, M.K. Afzal, M. Ateeq, S.W. Kim, Y.B. Zikria, Intelligent learning automata-based objective function in RPL for IoT, Sustainable Cities Soc. 59 (2020) 102234, http://dx.doi.org/10.1016/j.scs.2020.102234, URL http://www.sciencedirect.com/science/article/pii/S2210670720302213.

[5] M.K. Afzal, M.H. Rehmani, Y.B. Zikria, Q. Ni, Data-driven intelligence in wireless networks: Issues, challenges, and solution, Trans. Emerg. Telecommun. Technol. 30 (8) (2019) e3722, http://dx.doi.org/10.1002/ett.3722.

[6] T.R. G, S.P. R.M, P. M., C.L. Chowdhary, P.K.R. M, S. Hakak, W.Z. Khan, A deep neural networks based model for uninterrupted marine environment monitoring, Comput. Commun. 157 (2020) 64–75, http://dx.doi.org/10.1016/j.comcom.2020.04.004, URL http://www.sciencedirect.com/science/article/pii/S0140366420300542.

[7] F. Al-Turjman, M.H. Nawaz, U.D. Ulusar, Intelligence in the Internet of Medical Things era: A systematic review of current and future trends, Comput. Commun. 150 (2020) 644–660, http://dx.doi.org/10.1016/j.comcom.2019.12.030, URL http://www.sciencedirect.com/science/article/pii/S0140366419313337.

[8] S.A. Haider, M.N. Adil, M. Zhao, Optimization of secure wireless communications for IoT networks in the presence of eavesdroppers, Comput. Commun. 154 (2020) 119–128, http://dx.doi.org/10.1016/j.comcom.2020.02.027, URL http://www.sciencedirect.com/science/article/pii/S0140366419311946.

[9] Y. Chen, B. Song, X. Du, N. Guizani, The enhancement of catenary image with low visibility based on multi-feature fusion network in railway industry, Comput. Commun. 152 (2020) 200–205, http://dx.doi.org/10.1016/j.comcom.2020.01.040, URL http://www.sciencedirect.com/science/article/pii/S0140366419312733.

[10] O. Irshad, M.U.G. Khan, R. Iqbal, S. Basheer, A.K. Bashir, Performance optimization of IoT based biological systems using deep learning, Comput. Commun. 155 (2020) 24–31, http://dx.doi.org/10.1016/j.comcom.2020.02.059, URL http://www.sciencedirect.com/science/article/pii/S0140366419312782.

[11] R. Ali, B. Kim, S. Kim, H. Kim, F. Ishmanov, (ReLBT): A Reinforcement learning-enabled listen before talk mechanism for LTE-LAA and Wi-Fi coexistence in IoT, Comput. Commun. 150 (2020) 498–505, http://dx.doi.org/10.1016/j.comcom.2019.11.055, URL http://www.sciencedirect.com/science/article/pii/S0140366419313489.

[12] M. Masud, G. Muhammad, H. Alhumyani, S.S. Alshamrani, O. Cheikhrouhou, S. Ibrahim, M.S. Hossain, Deep learning-based intelligent face recognition in IoT-cloud environment, Comput. Commun. 152 (2020) 215–222, http://dx.doi.org/10.1016/j.comcom.2020.01.050, URL http://www.sciencedirect.com/science/article/pii/S0140366419312988.

[13] H. Khan, P.M. Shah, M.A. Shah, S. ul Islam, J.J. Rodrigues, Cascading handcrafted features and convolutional neural network for IoT-enabled brain tumor segmentation, Comput. Commun. 153 (2020) 196–207, http://dx.doi.org/10.1016/j.comcom.2020.01.013, URL http://www.sciencedirect.com/science/article/pii/S0140366419313040.

[14] M.A. Amanullah, R.A.A. Habeeb, F.H. Nasaruddin, A. Gani, E. Ahmed, A.S.M. Nainar, N.M. Akim, M. Imran, Deep learning and big data technologies for IoT security, Comput. Commun. 151 (2020) 495–517, http://dx.doi.org/10.1016/j.comcom.2020.01.016, URL http://www.sciencedirect.com/science/article/pii/S0140366419315361.